Una falla de seguridad, ahora parcheada, en Microsoft Outlook podía ser aprovechada por actores maliciosos para obtener acceso a contraseñas en formato hash del NT LAN Manager (NTLM) v2 al abrir un archivo especialmente manipulado.

El problema, identificado como CVE-2023-35636 (puntuación CVSS: 6.5), fue abordado por la empresa tecnológica como parte de sus actualizaciones de «Patch Tuesday» de diciembre de 2023.

> *«En un escenario de ataque por correo electrónico, un atacante podría explotar la vulnerabilidad al enviar el archivo especialmente manipulado al usuario y persuadirlo para que abra dicho archivo»,* expresó Microsoft en un aviso emitido el mes pasado.

En un escenario de ataque basado en la web, un atacante podría alojar un sitio web (o aprovechar un sitio comprometido que acepte o aloje contenido proporcionado por el usuario) que contenga un archivo especialmente creado para aprovechar la vulnerabilidad.

Dicho de otra manera, el atacante tendría que convencer a los usuarios de hacer clic en un enlace, ya sea insertado en un correo electrónico de phishing o enviado a través de un mensaje instantáneo, y luego engañarlos para que abran el archivo en cuestión.

CVE-2023-35636 tiene su origen en la función de intercambio de calendarios en la aplicación de correo electrónico Outlook, donde se genera un mensaje de correo electrónico malicioso al insertar dos encabezados, «Content-Class» y «x-sharing-config-url», con valores manipulados con el fin de exponer el hash NTLM del usuario durante la autenticación.

Dolev Taler, investigador de seguridad de Varonis, a quien se le atribuye el descubrimiento y reporte del fallo, señaló que los hashes NTLM podrían ser filtrados mediante el uso de Windows Performance Analyzer (WPA) y Windows File Explorer. Sin embargo, estos dos métodos de ataque aún no han sido corregidos.

> *«Lo que resulta interesante es que WPA intenta autenticarse mediante NTLM v2 a través de la web abierta»*, comentó Taler.
>
> *«Normalmente, NTLM v2 debería utilizarse al intentar autenticarse contra servicios internos basados en direcciones IP. Sin embargo, cuando el hash NTLM v2 atraviesa la internet abierta, queda vulnerable a ataques de relay y a intentos de fuerza bruta fuera de línea.»*

Este hallazgo se produce cuando Check Point reveló un caso de *«autenticación forzada»* que podría ser aprovechado para filtrar tokens NTLM de un usuario de Windows al engañar a la víctima para que abra un archivo malicioso de Microsoft Access.

Microsoft, en octubre de 2023, anunció planes para descontinuar el uso de NTLM en Windows 11 a favor de Kerberos, con el objetivo de mejorar la seguridad debido a que NTLM no es compatible con métodos criptográficos y es susceptible a ataques de relay.